

Application No. 10/089858

Docket No.: 10096-00002-US

AMENDMENTS TO THE CLAIMS

1. (currently amended) A method for producing forgery-proof documents or data records using a security module,

- whereby the security module generates a secret which remains unknown to a document producer and the document producer can not gain access to the secret which can only be encrypted by an authentication unit,
- whereby the secret, together with information that reveals details about the identity of the security module, is transferred in encrypted form to an authentication unit,
- whereby the authentication unit decrypts the secret, recognizes the identity of the security module and encrypts the secret, together with information on the identity of the document producer, in such a way that only a checking unit can carry out a decryption and then the authentication unit transmits these to the document producer,
- whereby the document producer transfers its own data to the security module,
- whereby the security module irreversibly links by hash encryption the secret with the data that the document producer itself has introduced, and
- whereby it is not possible to draw conclusions about the secret,

characterized in that the output value of the a double combination machine is used to form an irreversible hash and that hash value is output from the outlet valve, the double combination machine comprising a first combination machine and a second combination machine each of which combines a result value on the basis of two input values, the result of the irreversible linking of the secret with the data introduced by the document producer, the data introduced by the document producer itself as well as the encrypted information of the authentication unit all serve to form the document that is transmitted to the checking unit.

Application No. 10/089858

Docket No.: 10096-00002-US

2. (Original) The method according to Claim 1, characterized in that the additional information transferred by the authentication unit contains details on the identity of the document producer and on the period of validity of the documents generated by the document producer.
3. (currently amended) The method for checking the authenticity of a document, characterized in that the checking unit checks whether the result of an irreversible linking by hash encryption of a secret with data introduced by a document producer have been incorporated into the document, in that the checking unit decrypts the secret and additional information that were encrypted by an authentication unit, in that the checking unit irreversibly links the decrypted secret with the data introduced into the document by the document producer, in the same manner as a security module used to produce the forgery-proof document, and in that the checking unit compares the result of the irreversible linking that it has performed itself with the result of an irreversible linking that was performed by the document producer and incorporated into the document, and the output value of the a double combination machine is used to form an irreversible hash and that hash value is output from the outlet valve, and the double combination machine comprising a first combination machine and a second combination machine each of which combines a result value on the basis of two input values.
4. (Original) The method according to Claim 3, characterized in that the comparison determines whether data introduced into the document by the document producer has been forged.
5. (New) The method according to Claim 3, characterized in that the first combination

Application No. 10/089858

Docket No.: 10096-00002-US

machine combines the secret with the data contained in an identification register that unambiguously identifies the security module at a confirmation unit, the result value of the first combination machine is input into an encryption machine which uses the key from a key register to generate an encrypted result value that can only be decrypted by the authentication unit, the result value being output from the security module via a first data output port is transferred to the authentication unit, and wherein data from the document producer itself is introduced into the security module and combined with the second combination machine with the secret that is stored in an intermediate memory unit, the result value of the second combination machine being input into a hash machine which forms the hash value of the input value, and the resultant value being output from the security module via a data output port in order to be incorporated into the document.

6. (New) The method according to claim 1, characterized in that the first combination machine combines the secret with the data contained in an identification register that unambiguously identifies the security module at a confirmation unit, the result value of the first combination machine is input into an encryption machine which uses the key from a key register to generate an encrypted result value that can only be decrypted by the authentication unit, the result value being output from the security module via a first data output port is transferred to the authentication unit, and wherein data from the document producer itself is introduced into the security module and combined with the second combination machine with the secret that is stored in an intermediate memory unit, the result value of the second combination machine being input into a hash machine which forms the hash value of the input value, and the resultant value being output from the security module via a data output port in order to be incorporated into the document.